



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



065.016 Configuration Management Policy



**Version 2.3
October 5, 2018**

065.016 Configuration Management Policy	Current Version: 2.3
065.000 Application Development	Review Date: 10/05/2018

Revision History

Date	Version	Description	Author
12/16/2011	1.0	Effective Date	CHFS IT Policies Team Charter
10/5/2018	2.3	Review Date	CHFS OATS Policy Charter Team
10/5/2018	2.3	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	10/5/2018	Jennifer Harp	
CHFS Chief Information Security Officer (or designee)	10/5/2018	DENNIS E. LEBER	

065.016 Configuration Management Policy	Current Version: 2.3
065.000 Application Development	Review Date: 10/05/2018

Table of Contents

1	POLICY DEFINITIONS.....	4
2	POLICY OVERVIEW.....	5
2.1	PURPOSE	5
2.2	SCOPE	5
2.3	MANAGEMENT COMMITMENT.....	5
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
2.5	COMPLIANCE	5
3	ROLES AND RESPONSIBILITIES	5
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO)	5
3.2	CHIEF PRIVACY OFFICER (CPO)	6
3.3	SECURITY/PRIVACY LEAD	6
3.1	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL	6
3.2	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	6
4	POLICY REQUIREMENTS	6
4.1	BASELINE CONFIGURATION	6
4.2	CONFIGURATION CHANGE CONTROL	7
4.3	ACCESS RESTRICTIONS FOR CHANGE.....	7
4.4	CONFIGURATION SETTINGS	7
4.5	LEAST FUNCTIONALITY	7
4.6	INFORMATION SYSTEM COMPONENT INVENTORY	8
4.7	CONFIGURATION MANAGEMENT PLAN	8
4.8	SOFTWARE USAGE RESTRICTIONS AND USER INSTALLED SOFTWARE	8
5	POLICY MAINTENANCE RESPONSIBILITY	8
6	POLICY EXCEPTIONS	9
7	POLICY REVIEW CYCLE.....	9
8	POLICY REFERENCES	9

065.016 Configuration Management Policy	Current Version: 2.3
065.000 Application Development	Review Date: 10/05/2018

1 Policy Definitions

- **Agency:** For the purpose of this document, agency or agencies refers to any department under CHFS.
- **Baseline Configuration:** Per the National Institute of Standards and Technology, it is a set of specifications for a system, or configuration item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual's tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual's personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother's maiden name, etc.).
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

065.016 Configuration Management Policy	Current Version: 2.3
065.000 Application Development	Review Date: 10/05/2018

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through a configuration management policy. This document establishes the agency's Application Configuration Management Policy to manage risks and provide guidelines for security best practices regarding configuration management.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

065.016 Configuration Management Policy	Current Version: 2.3
065.000 Application Development	Review Date: 10/05/2018

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.1 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section [8 Policy References](#) below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.2 System Data Owner and System Data Administrators

Management/lead who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

4 Policy Requirements

4.1 Baseline Configuration

CHFS agencies follow the Commonwealth Office of Technology (COT) [OIS-053 Windows and ESX Baseline Configuration Documentation Annual Review Procedure](#). This finalized process establishes the baseline security configuration for all windows systems supported by the COT windows Server Support Team.

065.016 Configuration Management Policy	Current Version: 2.3
065.000 Application Development	Review Date: 10/05/2018

CHFS follows Enterprise [OIS-051 Security Configuration Documentation Annual Review Procedure](#) by reviewing baselines and updates for desktop, laptop and printer components annually and during critical system patches, emergency patches, and/or major system updates, as required. COT is responsible for retaining older versions of baseline configurations for CHFS agencies servers, laptops, desktops, printers, network switches, and firewall components. The CHFS agencies will retain configurations, current and past versions, for software components.

4.2 Configuration Change Control

CHFS agencies follow the [CHFS 010.103- Change Control Policy](#) and [CHFS 065.014- CHFS SDLC and New Application Development Policy](#) regarding change control guidelines. The CHFS agencies and/or the enterprise will retain records of configuration-controlled changes to the Information System for a minimum of three (3) years.

4.3 Access Restrictions for Change

To ensure the completion of software application update reviews and implementation the following policies/procedure are followed by CHFS agencies to document significant changes to software, hardware, communication links, and operational procedures:

- [Enterprise Policy CIO-101 Enterprise Release Management Policy.](#)
- [Enterprise Procedure: COT-067- Enterprise Security Standard Process and Procedures Manual \(ESSPPM\) Section 5.7.6- Hardware Changes/Configuration Management](#)
- [Enterprise Procedure: COT-009 Change Management](#)

4.4 Configuration Settings

CHFS agencies will follow COT security configuration guidelines, which include mandatory baseline configuration settings for information systems. Any exceptions from these mandatory configurations must go through the formal CHFS approval process by following [CHFS 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls Policy](#), or the formal COT [Security Exemption Request, COT-F085](#) form process.

4.5 Least Functionality

CHFS agencies are required to configure roles granting system access based on the principle of least privilege. COT prohibits and disables the use of high-risk system services, ports, network protocols, and capabilities across network boundaries that are not explicitly required for system or application functionality. COT supports the entire Commonwealth infrastructure for the agencies.

COT performs monthly vulnerability scans of networks, servers and databases to identify unnecessary functions, ports, protocols and/or services. Based on the scanning results, COT coordinates with necessary agency personnel to remediate/disable unnecessary functions, ports, protocols, and/or services identified.

065.016 Configuration Management Policy	Current Version: 2.3
065.000 Application Development	Review Date: 10/05/2018

4.6 Information System Component Inventory

COT shall utilize the Procurement, Payables, and Asset Tracking System (PPATS) for tracking IT hardware assets through their lifecycle from procurement to disposal. Along with the PPATS system, COT Asset Management Division maintains an up-to-date inventory of software under its control for quality assurance.

4.7 Configuration Management Plan

OATS IS Team recommends each agency to develop, document, and implement a configuration management plan for the information system. This plan shall include, but is not limited to:

- Addressing roles, responsibilities, configuration management processes, and procedures;
- Establishing a process for identifying configuration items throughout the systems development lifecycle (SDLC) and managing the configuration of items;
- Defining configuration items for information systems and place the configuration items under configuration management;
- Protecting the configuration management plan from unauthorized disclosure and modification;

National Institute of Standards and Technology (NIST) Special Publication 800-128 Revision 1, Guide for Security-Focused Configuration Management of Information Systems- Appendix D can be referenced and used as a guide/sample for agencies when creating a configuration management plan.

4.8 Software Usage Restrictions and User Installed Software

COT Division of Asset Management is responsible for periodically reviewing compliance of software licenses and copyright policies. Additionally, each COT department's management is responsible for ensuring that the necessary documentation is available to provide proof of proper software acquisition.

COT-067: ESSPPM, Section 3- Logical Security Processes and Procedures ensures standardized configurations for hardware and software. For security reasons, installation of unauthorized applications are not permitted on the network. Any unauthorized applications will be removed and the use may be subject to disciplinary actions.

Any exceptions from these mandatory configurations must go through the formal CHFS approval process by following the Enterprise Kentucky Information Technology Standards (KITS) Exception Request Form, COT-027, or the formal COT exception process following Security Exemption Request, COT-F085.

5 Policy Maintenance Responsibility

The CHFS OATS IS Team is responsible for the maintenance of this policy.

065.016 Configuration Management Policy	Current Version: 2.3
065.000 Application Development	Review Date: 10/05/2018

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 010.103- Change Control Policy
- CHFS OATS Policy: 065.014 CHFS SDLC and New Application Development Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS Procurement, Payables, and Assets Tracking System (PPATS)
- Enterprise IT Policy: CIO-101- Enterprise Release Management Policy
- Enterprise IT Procedure: COT-067: Enterprise Security Standard Process and Procedures Manual (ESSPPM)
- Enterprise IT Procedure: OIS-051- Security Configuration Documentation Annual Review Procedure for Printers, Desktops, and Laptops Procedure
- Enterprise IT Procedure: OIS-053- Windows and ESX Baseline Configuration Documentation Annual Review Procedure
- Enterprise Security Exemption Request, COT-F085
- Enterprise Kentucky Information Technology Standards (KITS) Exception Request Form, COT-027
- Internal Revenue Services (IRS) Publication 1075
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- National Institute of Standards and Technology (NIST) Special Publication 800-128 Revision 1, Guide for Security-Focused Configuration Management of Information Systems
- Social Security Administration (SSA) Security Information